MG-R(SVR)
Technical Guidance

- General Description of How MG-R(SVR) Technology Works -

April 6, 2004

Toshiya Kaihoko
Senior Engineer
Personal Audio Company, IT & Mobile Network Company

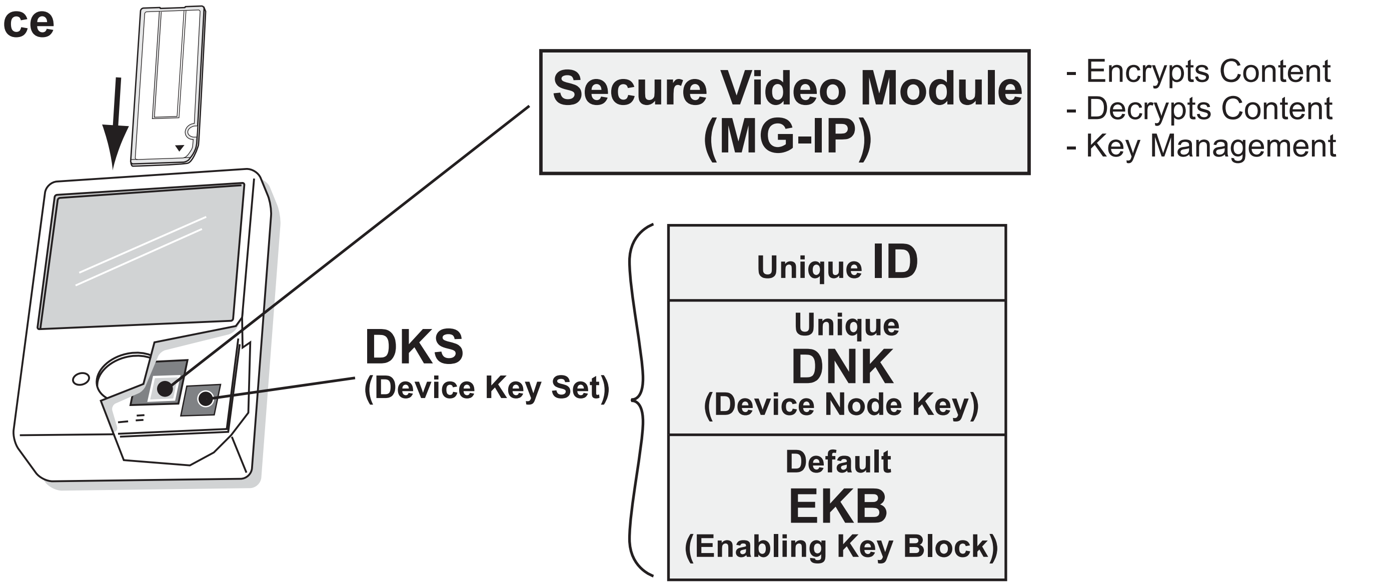
Sony Corporation

MG-R(SVR)
Technical Guidance

1. Requirements for Media and Devices
2. Content Recorded With MG-R(SVR)
3. Retrieving Common Key with EKB and DNK
4. Revocation Using Renewed EKB
5. Procedure of Recording Content
6. Procedure of Playing Back Content
7. Propagation of New EKB Files to Revoke DNKs
8. Secure Authenticated Channel
9. Method of Binding Content to the Medium
10. Prevention of Re-transmission to the Internet
11. Renewal of Software Secure Video Module
12. Hi-MD 1GB and Hi-MD 300MB Media

Requirements for Media and Devices

MG-R(SVR) Device



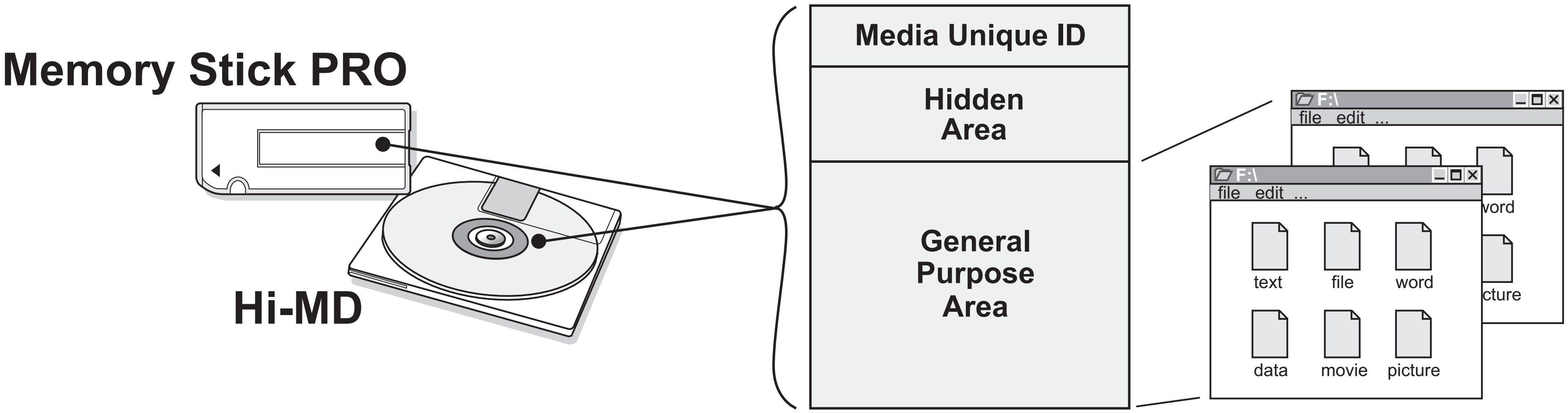
Secure Video Module (MG-IP)

- Encrypts Content
- Decrypts Content
- Key Management

DKS (Device Key Set)

Unique **ID**
Unique **DNK** (Device Node Key)
Default **EKB** (Enabling Key Block)

MG-R(SVR) Media



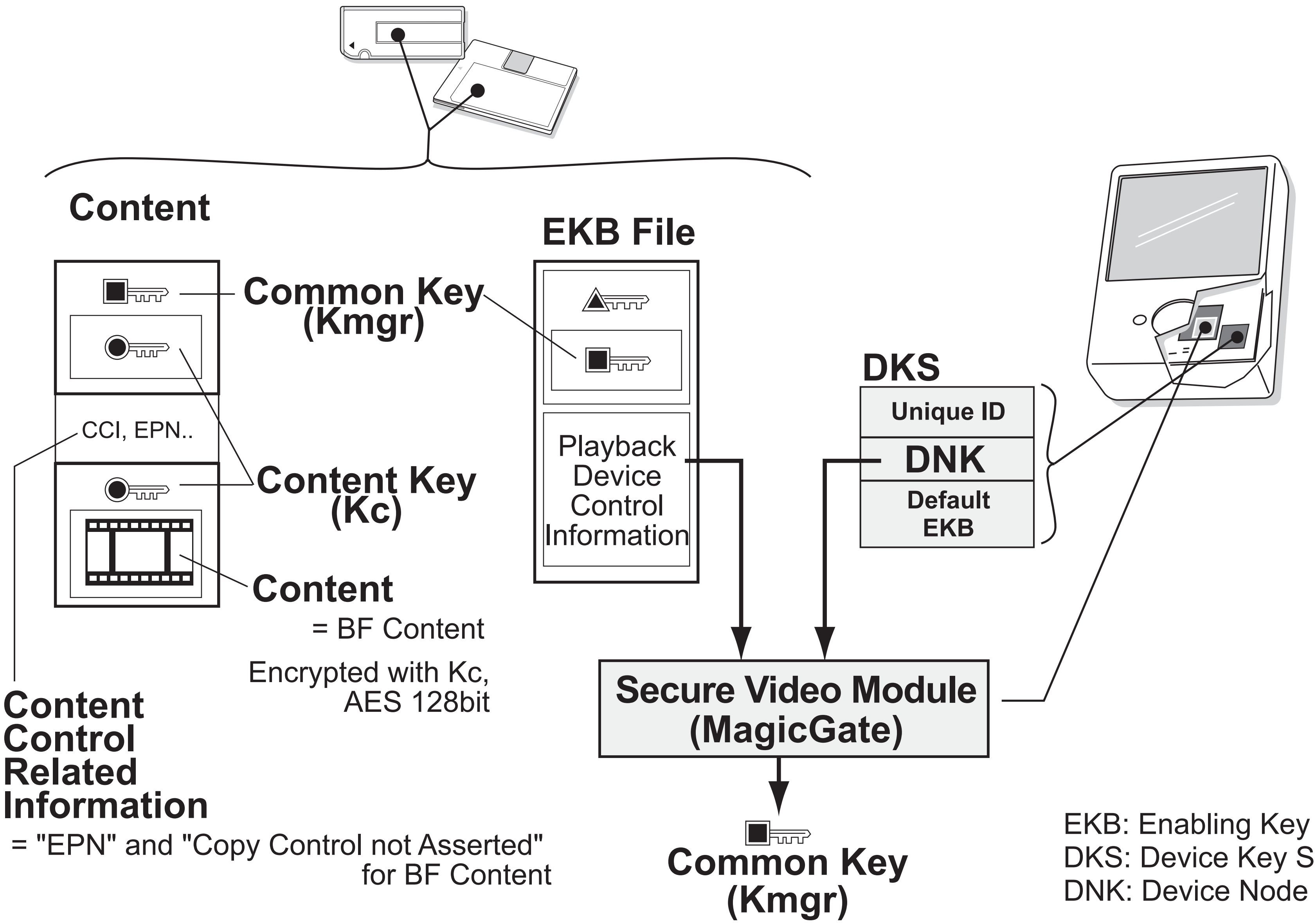
Memory Stick PRO

Hi-MD

Media Unique ID
Hidden Area
General Purpose Area

For details, see Section 3,4 and 5, Figure 1 and 2 in the Technical Guidance Document

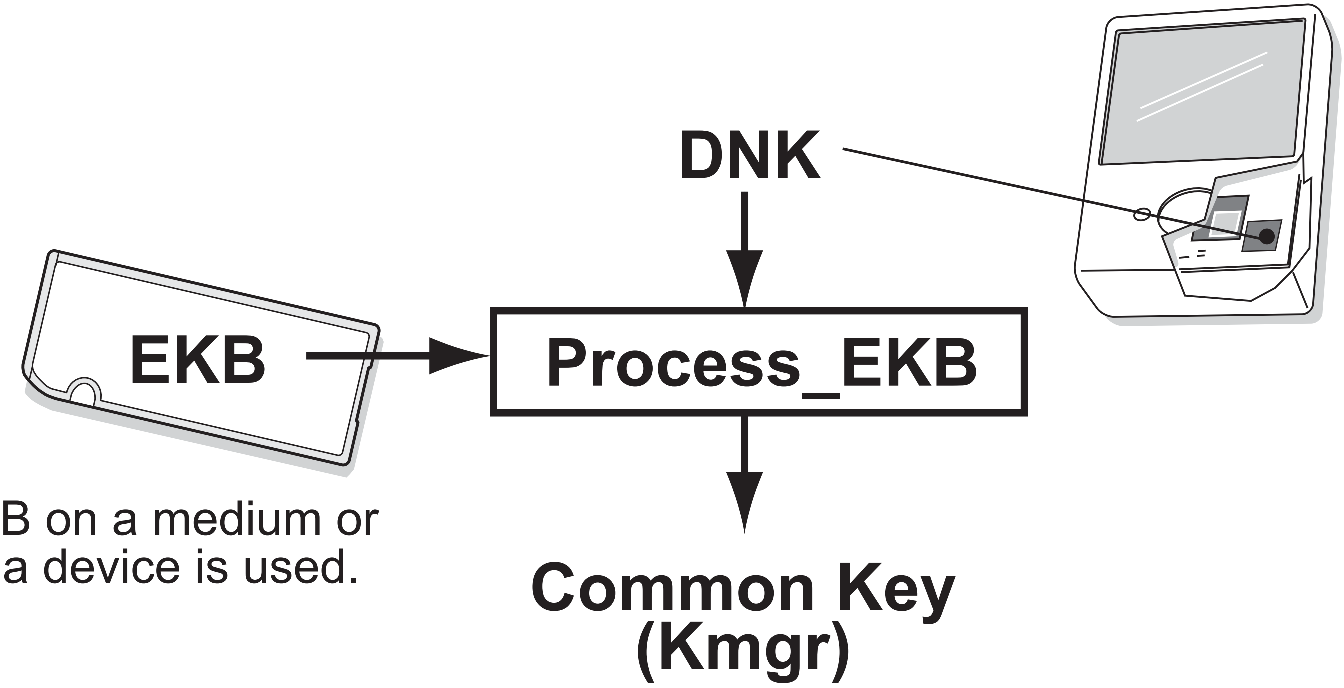
Content Recorded With MG-R(SVR)



EKB: Enabling Key Block
DKS: Device Key Set
DNK: Device Node Key

For details, see Section 8 and Figure 6 in the Technical Guidance Document

Retrieving Common Key with EKB and DNK



DNK

EKB

Process_EKB

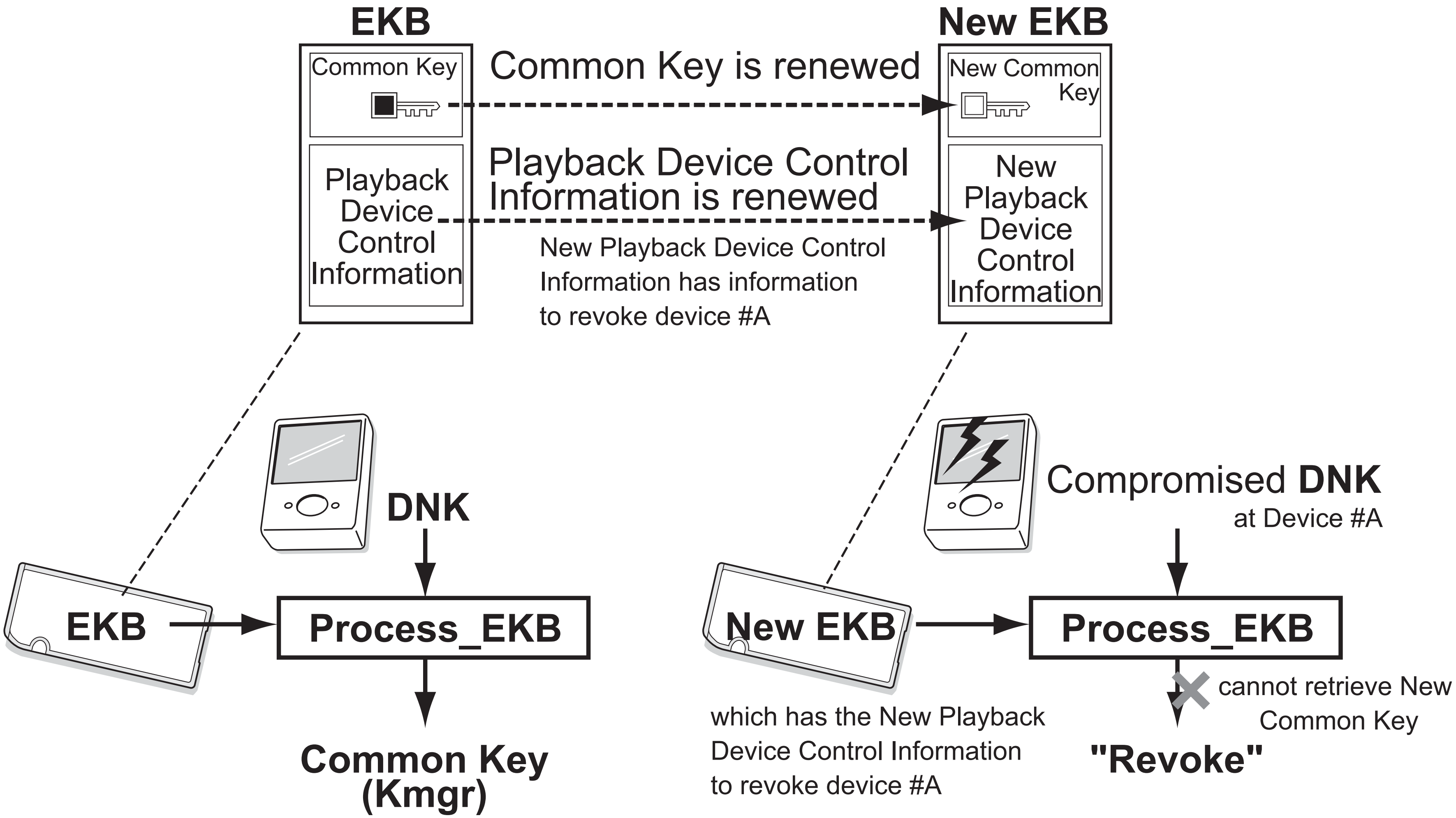
Common Key
(Kmgr)

EKB on a medium or
on a device is used.

EKB: Enabling Key Block
DNK: Device Node Key

For details, see Section 9 and Figure 7 in the Technical Guidance Document
See also Section 5 and Figure 5.1 in the MG-R(SVR) Specification - Informational Version

Revocation using Renewed EKB



EKB

Common Key

Playback Device Control Information

Common Key is renewed

Playback Device Control Information is renewed

New Playback Device Control Information has information to revoke device #A

New EKB

New Common Key

New Playback Device Control Information

DNK

EKB

Process_EKB

Common Key (Kmgr)

Compromised **DNK** at Device #A

New EKB

Process_EKB

which has the New Playback Device Control Information to revoke device #A

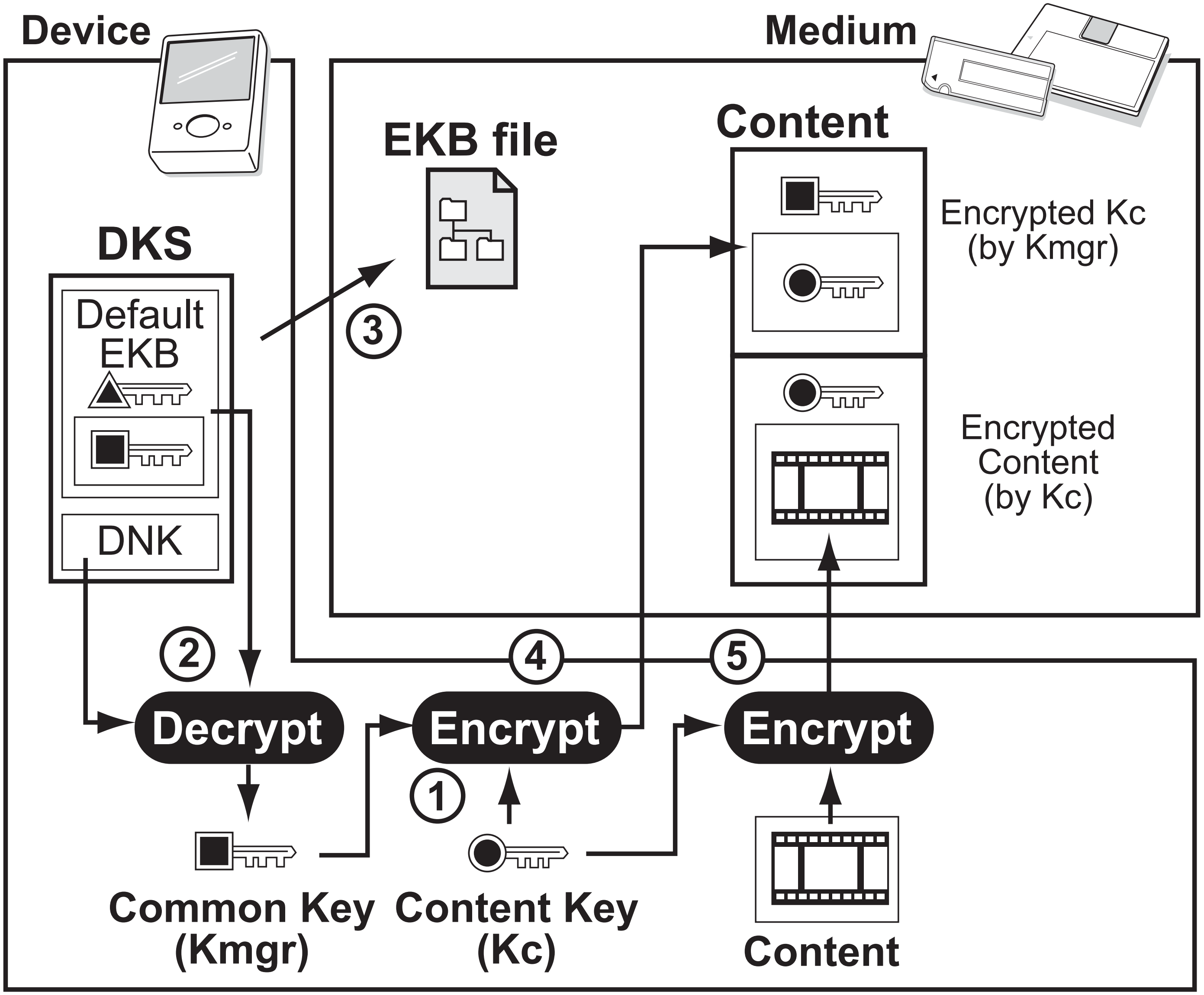
cannot retrieve New Common Key

"Revoke"

EKB: Enabling Key Block
DNK: Device Node Key

For details, see Section 10 and Figure 8 in the Technical Guidance Document
See also Section 5 and Figure 5.2 in the MG-R(SVR) Specification - Informational Version

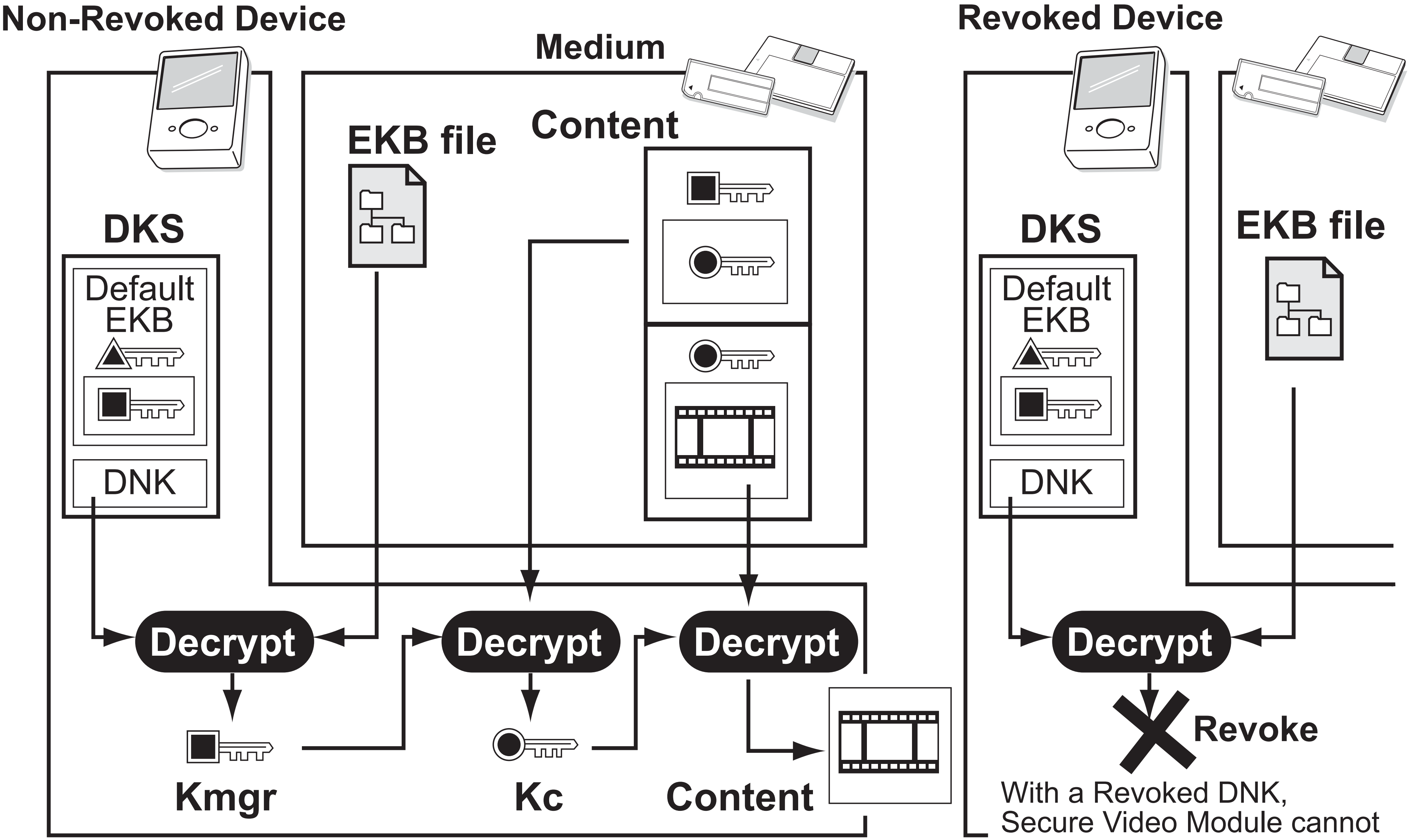
Procedure of Recording Content



EKB: Enabling Key Block
DKS: Device Key Set
DNK: Device Node Key

For details, see Section 11.1 and Figure 9 in the Technical Guidance Document

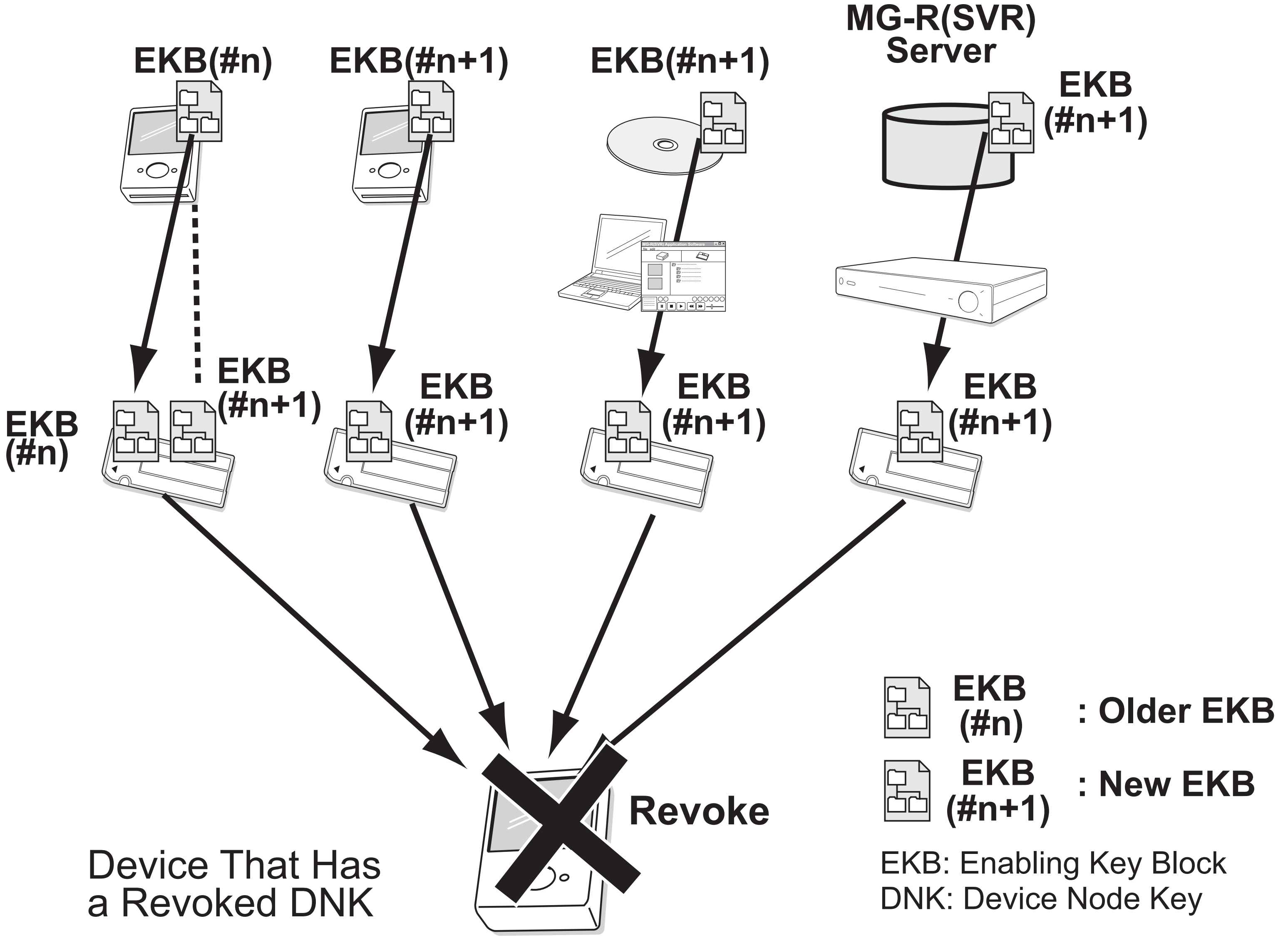
Procedure of Playing Back Content



With a Revoked DNK,
Secure Video Module cannot
retrieve the Common Key(Kmgr)
and therefore cannot obtain the
Content Key. This means it is Revoked.

For details, see Section 11.2 and Figure 10 in the Technical Guidance Document

Propagation of New EKB Files to Revoke DNKs



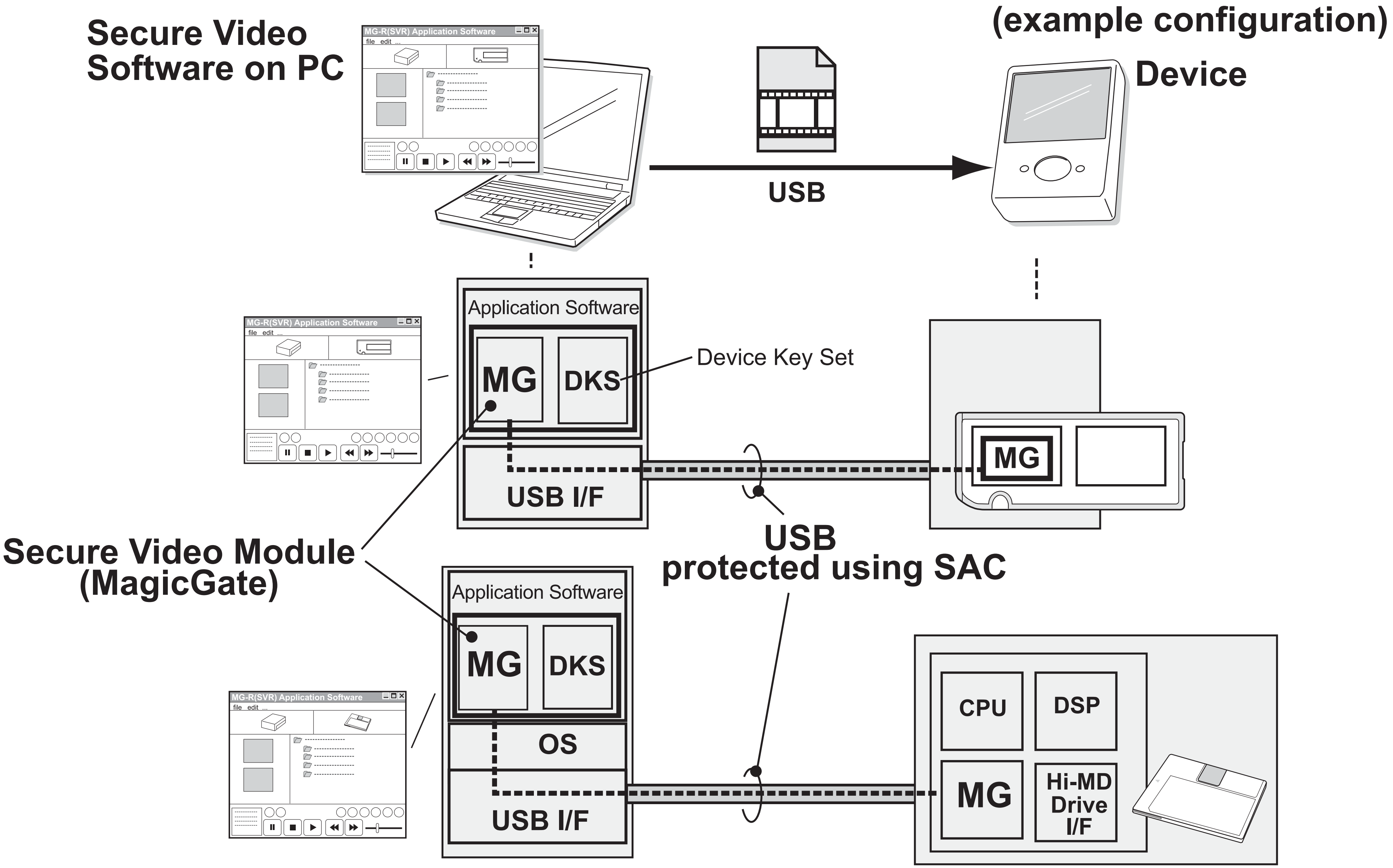
EKB (#n) : Older EKB

EKB (#n+1) : New EKB

EKB: Enabling Key Block
DNK: Device Node Key

For details, see Section 12 and Figure 11 in the Technical Guidance Document

Secure Authenticated Channel



Secure Video Software on PC

(example configuration)

Device

USB

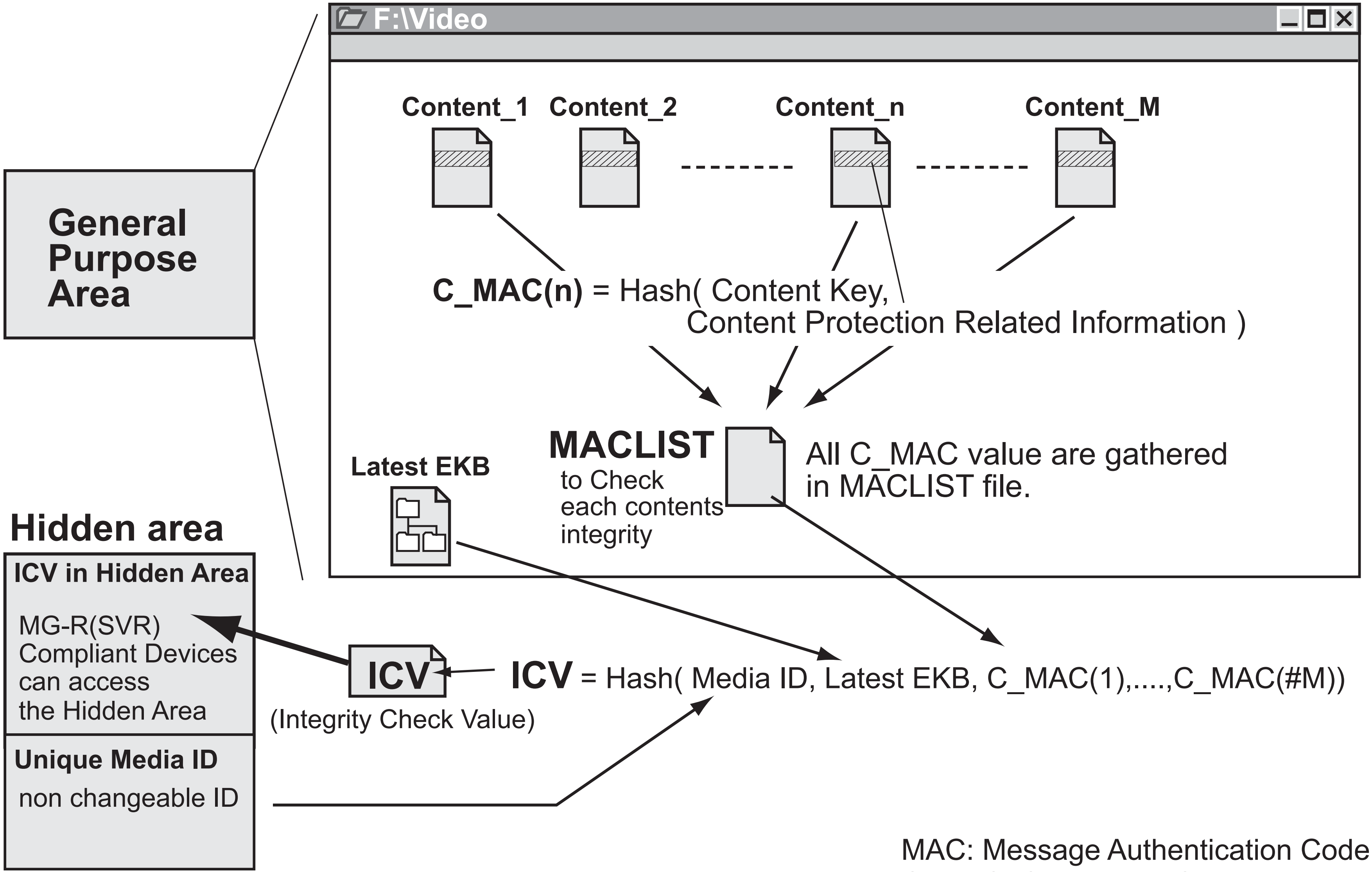
Device Key Set

Secure Video Module (MagicGate)

USB protected using SAC

For details, see Section 7 and Figure 5 in the Technical Guidance Document

Method of Binding Content to the Medium



General Purpose Area

F:\Video

Content_1 Content_2 Content_n Content_M

C_MAC(n) = Hash(Content Key, Content Protection Related Information)

MACLIST to Check each contents integrity

All C_MAC value are gathered in MACLIST file.

Latest EKB

Hidden area

ICV in Hidden Area

MG-R(SVR) Compliant Devices can access the Hidden Area

Unique Media ID

non changeable ID

ICV

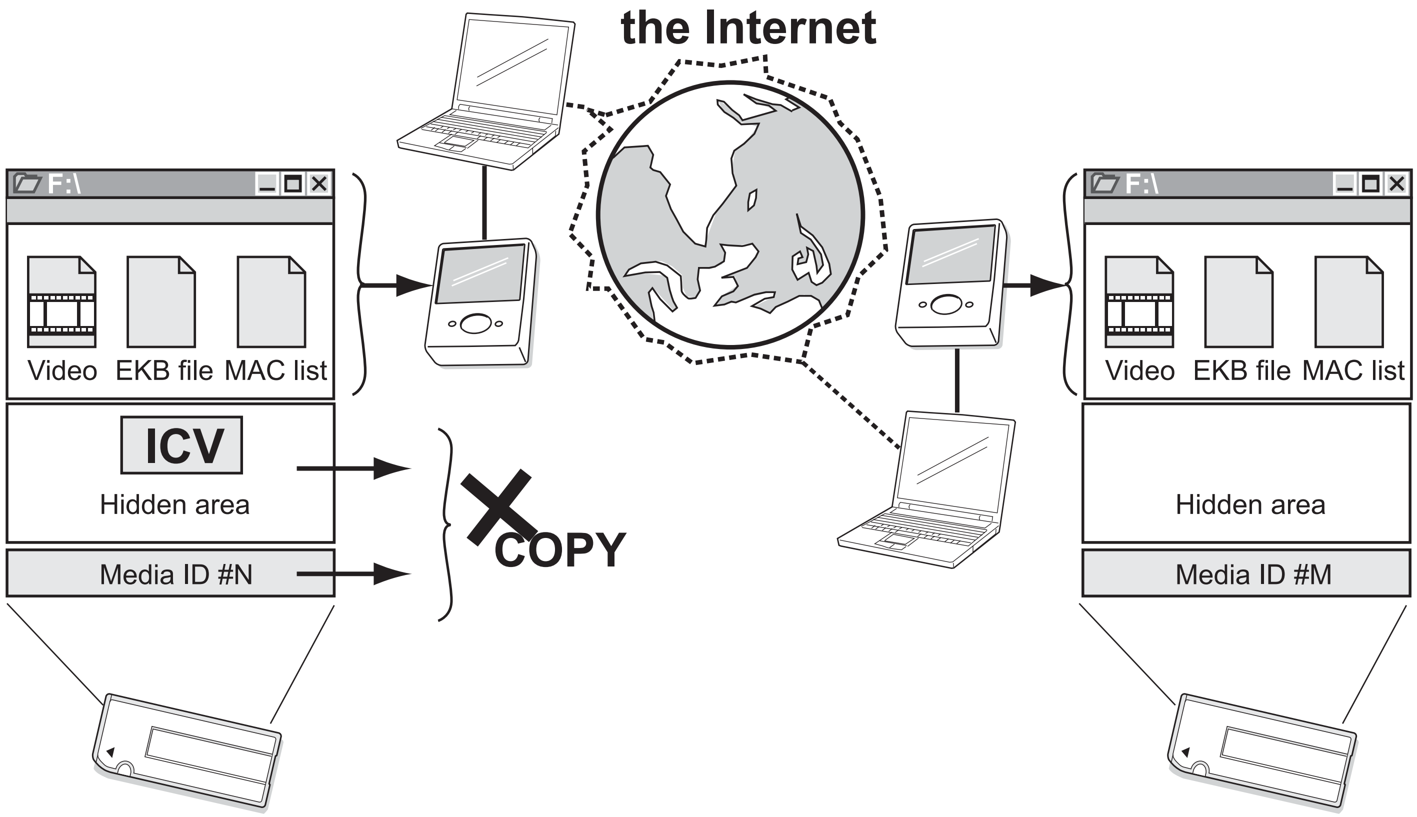
(Integrity Check Value)

ICV = Hash(Media ID, Latest EKB, C_MAC(1),....,C_MAC(#M))

MAC: Message Authentication Code
C_MAC: Content MAC
ICV: Integrity Check Value
EKB: Enabling Key Block

For details, see Section 13 and Figure 12 in the Technical Guidance Document

Prevention of Re-transmission to the Internet



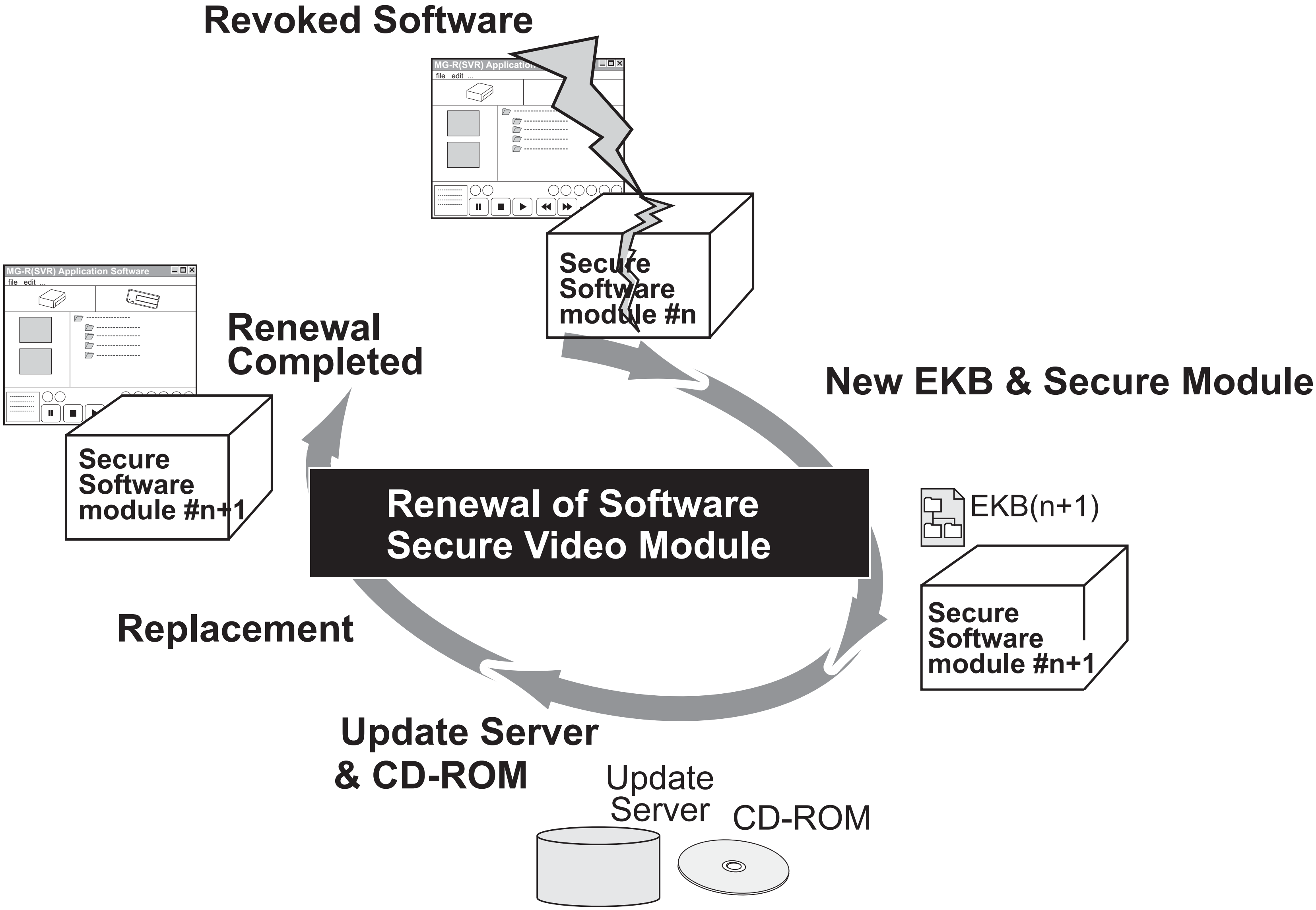
Different Media ID and No ICV, Therefore Integrity Check Fails and Playback is Blocked

ICV: Integrity Check Value
EKB: Enabling Key Block

For details, see Section 14 and Figure 13 in the Technical Guidance Document

Renewal of Software Secure Video Module

(software implementation only)



Revoked Software

Secure Software module #n

New EKB & Secure Module

EKB(n+1)

Secure Software module #n+1

Update Server & CD-ROM

Update Server

CD-ROM

Replacement

Renewal Completed

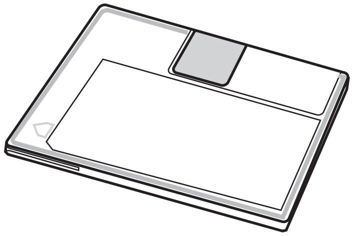
Secure Software module #n+1

Renewal of Software Secure Video Module

For details, see Section 15 Figure 13 in the Technical Guidance Document

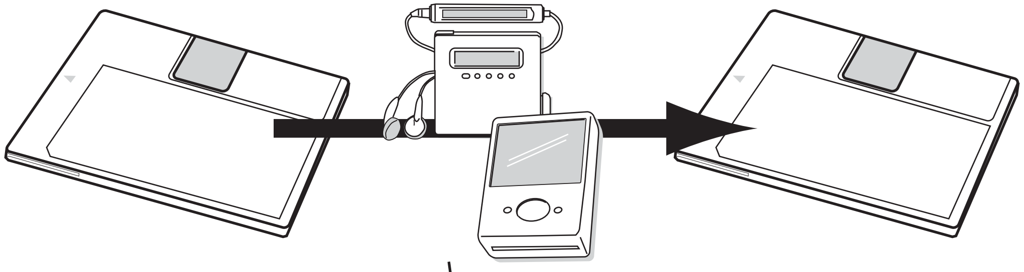
Hi-MD 1GB and Hi-MD 300MB media

Hi-MD media are categorized in two types, and their Media Unique IDs are written as follows:



Hi-MD 1GB

Media Unique ID is written onto a Hi-MD 1GB medium when it is produced by a licensee of MG-R(SVR) for Hi-MD media



MiniDisc (for Audio)

Hi-MD 300MB

Compliant Device writes the Media Unique ID onto a Hi-MD 300MB when formatting it. Media Unique ID is never changed (except when media are formatted, which erases all content)

All Hi-MD Compliant Devices can format MiniDisc media as Hi-MD 300MB media

For details, see Section 3 in the MG-R(SVR) for Hi-MD - Technical Guidance Document

Summary

- Each MS PRO or Hi-MD medium has a Media Unique ID and a Hidden Area
- Hidden Area can be accessed only by MG-R(SVR) Compliant Devices
- Device has a Secure Video Module and a Device Key Set
- Content is encrypted by the Content Key (Kc);
  Content Key is encrypted by the Common Key (Kmgr);
  Common Key is retrieved from EKB (Enabling Key Block) and DNK (Device Node Key)
- SAC (Secure Authenticated Channel) protects secure information transferred on USB
- Content is protected from alteration using Integrity Check Value (ICV): a hash of content data, content protection related information, and Media Unique ID
- ICV stored in Hidden Area also prevents illegal retransmission of the content
- Content cannot be copied bit-by-bit (such copies will not play)
- Media Unique ID on Hi-MD 300MB is written by Hi-MD Devices, but is never changed except when being formatted